Testimony for the Record
Submitted to the House Committee on Financial Services
Subcommittee on Oversight and Investigations
Hearing on "Fraud in Focus: Exposing Financial Threats to American Families"
September 18, 2025

Kate Griffin
Director, National Task Force on Fraud and Scam Prevention
The Aspen Institute Financial Security Program

Chairman Meuser, Ranking Member Green, and distinguished members of the Subcommittee,

Thank you for inviting me to testify today on an issue that is presenting a threat to our national security, to the systems of communication, commerce, and finance in our country, and to Americans' household financial security: Scams - the ability of criminals to deploy sophisticated technological tools and psychological warfare to socially engineer everyday consumers into sending money and personal information.

The United States is caught in a global conflict with these scammers and we are not yet winning. Working mostly from safe havens overseas, criminals are exploiting America's communications, banking, and digital platforms to deceive Americans into sending money, divulging sensitive information, or worse. A majority of Americans say they get scam calls, emails, and texts at least weekly, and more than 50 million U.S. adults have lost money to an online scam or attack. This causes American households to lose more than two billion dollars *every week,* among other harms. Often, scammers are part of transnational criminal organizations that use fraud and scams to fund other crimes, including drug and human trafficking. In addition to lowering criminals' barriers to entry, cryptocurrency and artificial intelligence-powered deepfakes are fueling the scams boom, enabling ever-faster and more powerful forms of criminal deceit.

Over the last year, the Aspen Institute Financial Security Program (Aspen FSP) has convened the **National Task Force for Fraud and Scam Prevention** to bring together parties with an interest in stopping this crime, protecting consumers, and restoring trust in our systems. During that time, at least 300 experts from more than 80 organizations – including some of the largest companies on the frontlines against scammers, such as JPMorgan Chase, Google, Target, Microsoft, Verizon, Amazon, and Meta – contributed thousands of hours to it.[i] It is the first time such a broad collection of leaders from

government, law enforcement, private industry, and civil society have come together in the United States to help develop a strategy aimed at preventing fraud and scams.

My testimony today reflects the insights gained from the Task Force and summarizes key recommendations from Aspen FSP based on this experience, which we will soon publish in a major new report. We believe that America can fix the scam problem by deploying the best of the American spirit: bold leadership, innovative thinking, and well-coordinated effort.

Overview of the Scams Threat

Scams are a whole-of-society threat to America

- 1 in 5 U.S. adults (53 million) claim they lost money to an online scam or attack.[ii]
- Among victims who lost money to scams or online attacks, three-quarters have never filed reports with law enforcement.[iii] Victims cite confusing procedures, shame, and hopelessness as reasons for not seeking help from authorities.[iv]
- Still, FBI and FTC complaints document about $16 billion and $12 billion in annual losses, respectively, and the FTC estimates that actual fraud-related losses to U.S. consumers, accounting for under-reporting, exceed $158 billion per year.[v]
- Bipartisan majorities of U.S. adults say the federal government is doing a "bad job" handling online scams and attacks.[vi]
- Research suggests that the scams industry now rivals the size of the illicit drug trade and is growing fast.[vii] Scam losses reported to law enforcement have more than tripled since 2019.[viii]
- Everyone is at risk of becoming a scam victim.[ix] Younger adults report experiencing scams in their households more than older adults, while older adults report losing about twice as much money when they are scammed.[x]

Text, phone, email, social media, and financial systems in America are at risk

- Most U.S. adults report receiving scam messages daily or weekly through phone (68%), email (63%), or text (61%) and 33% report the same through social media.[xi]

- 6 in 10 Americans or more say online scams are a “major problem” on text and phone, email, and social media, while roughly half say the same about shopping, banking, and payment sites or apps.[xii]

- Being tricked by a scammer to send money or provide access to a financial account is the second-largest crime concern in the U.S. (57% of adults worry about it).[xiii]

- Victims rarely report financial fraud to law enforcement: Most victims (7 in 10) reported directly to their financial institutions, while only 1 in 10 reported to local law enforcement and 1 in 17 reported to a federal agency.[xiv]

Scams are a national security threat and a national priority

- The Annual Threat Assessment of the U.S. Intelligence Community has identified scams as part of a nexus of “criminal activity threatening the United States” perpetrated by Transnational Criminal Organizations (TCOs) and state-affiliated groups that also engage in human trafficking, drug trafficking, and weapons and human smuggling.[xv] But to date, officials have not designated scams against American households as a discreet threat or target for disruption.

- North Korean hackers, Mexican cartels, Russian crime syndicates, and Triad gangs are among the U.S. adversaries that benefit from scams and other financial crimes.[xvi]

- U.S. Department of the Treasury’s Office of Foreign Assets Control has imposed sanctions state & non-state sponsored TCOs for scam related activity, including Southeast Asian Networks operating in Shwe Kokko, Burma, a notorious hub for virtual currency investment scams under the operational control of the OFAC-designated Karen National Army (KNA)[xvii], The Zhao Wei Transnational Criminal Organization operating in the illusive scam compound at the border of Myanmar, Laos, and Thailand, also known as The Golden Triangle Special Economic Zone[xviii], and The Lazarus Group, which has ties to the North Korean government, channels revenues generated from fraud and scams to the regime[xix]. The FBI has issued warnings about The Jalisco New Generation Cartel running scam call centers that finance narcotics trafficking and money laundering.[xx]

More information on scam trends can be found in the appendix.

Transnational Scams Require a Paradigm Shift for Law Enforcement and Intelligence

The escalating threat of transnational criminal organizations (TCOs) operating overseas while interacting digitally with millions of U.S. consumers fundamentally redefines criminal behavior. This demands a paradigm shift in the national response.

Traditional civil law enforcement tactics, such as domestic lawsuits and domestic asset freezing, often have little deterrence effect against such overseas criminals. Similarly, domestic criminal law enforcement approaches, traditionally focused on post-facto investigation and prosecution, can be overwhelmed by the challenge of protecting people and property against the high-tech, high-speed, high-volume global threat that scammers represent.

To counter this challenge effectively, government responses must evolve. Increasing the nation's capability to stop scams before they happen requires policies that drive a pivot toward preventing financial crime. Law enforcement agencies will have to become more focused on disrupting scam criminals. The U.S. Intelligence Community will have to prioritize detecting transnational scam activity and working to protect Americans from it. All agencies will have to become more coordinated and share more actionable scam intelligence with each other and with companies; and they will have to increase their capacity to analyze information and act on it to effectively counter the speed and technical sophistication of transnational scam criminals.

A Call to Respond

Companies and government agencies are expending extraordinary effort to fight scams against consumers. They have had some success, and the recommendations in the forthcoming report reflect lessons they have learned. But more is needed. The scams threat continues to grow as large volumes of criminals use rapidly evolving tactics to challenge the limits of our systems.

A ***whole-of-ecosystem*** response is urgently needed to undermine the criminal scam business model, strengthen systems, and protect consumers.

The national response must emphasize government and private sector collaboration.

- **Corporate leaders** must act decisively to suppress scam activity at every stage of its lifecycle. They must empower staff with resources and guidance to maintain robust anti-scam policies and respond effectively when scams occur.

- **Policymakers** must act boldly to enable the required response. **Congress** and the **White House** should recognize scams as a national security threat and priority. They must empower a comprehensive private sector response by enhancing incentives and modernizing legal frameworks; and they must drive better law enforcement and intelligence outcomes by tasking top officials with clear anti-scam goals, backed by sufficient funding and cross-jurisdictional authority.

Corporate Recommendations

Companies in sectors targeted or exploited by scammers, including telecommunications, messaging, digital platforms (social media, paid advertising, and retail), and financial services (banking, fintech, payments, and crypto) should:

- **Maintain robust anti-scam policies addressing the entire scam lifecycle.** C-suite level leaders should own these policies and include accountability mechanisms, adequate budget allocations, and clear expectations for customer service and data protection.
- **Strengthen system defenses.** Improve identity verification and authentication to block inauthentic actors, including evaluating the trustworthiness of advertisers and merchants. Use technology such as liveness testing and interoperable digital credentials to disrupt non-authentic communications.
- **Enhance capabilities to detect suspicious activity.** Invest in private information exchanges with companies in other sectors. Help improve standards for interoperability and ethical governance. Direct legal counsel to establish suitable compliance policies or seek necessary regulatory guidance or safe harbors.
- **Disrupt scams in process.** Take reasonable steps against suspicious activity based on actionable scam intelligence. Take down fraudulent communications channels (e.g. websites), deactivate accounts and profiles of bad actors, and dismantle scammer infrastructure. Continuously improve just-in-time warnings and interventions for customers.
- **Improve reporting and recovery mechanisms.** Share more actionable scam intelligence with law enforcement agencies. Promote effective recovery for victims by providing user-friendly reporting and dispute resolution mechanisms and ensuring fast correction of false positives or account takeovers (ATO).
- **Measure and evaluate interventions.** Pilot the proposed metrics framework for scams and report on results.[xxi]
- **Collaborate with peers to strengthen scam defenses**. Share best practices across relevant industry sectors and advocate for policy improvements.

Public Policy and Government

The federal government and law enforcement and intelligence agencies, alongside state counterparts, should:

- **Elevate scam prevention as a national priority.** Starting with the White House and Congress, recognize scams as a national security threat and make scam prevention a whole-of-government priority. Establish a national strategy to combat scams, with dedicated resources and broad coordination mechanisms, such as a Congressional Commission or an administrative czar or division with whole-of-government authority. Empower and direct law enforcement and intelligence agencies to improve scam prevention outcomes.
- **Enhance incentives and modernize legal frameworks for combating scams**. Clarify duties for companies to prevent scam activity and de-risk participation in scam suppression efforts, by enacting "good Samaritan" liability protections for companies acting reasonably and in good faith.
- **Enhance law enforcement capabilities.** Increase statutory powers for asset seizure and recovery across all forms of money movement (including digital assets) and punishing transnational illicit financial activity. Create specialist anti-scam units, allocate resources, and develop training programs to improve recognition of scam activity and respond to it.
- **Combat cross-border financial crime.** Apply sanctions and use diplomatic tools against foreign governments and private parties that enable or benefit from scams. Formalize diplomatic engagements with allied nations to shut down scam centers. Improve intelligence gathering to disrupt transnational scam activity.
- **Modernize data collection and analysis.** Review and upgrade key law enforcement databases to improve data intake, analysis, and interoperability, leveraging modern technology like APIs and artificial intelligence (starting with FBI's Internet Crime Complaint Center (IC3), FTC Sentinel, and FinCEN's Suspicious Activity Reports (SARs) systems). Create a single portal (e.g. stopscams.gov) for companies to report scam intelligence, including mechanically or in bulk, with the system distributing inputs to the appropriate government databases. Enhance law enforcement analytical capabilities to identify trends and improve deconfliction across agencies.
- **Improve feedback loops**. Law enforcement agencies should publish regular analysis of scam trends and prosecutions to industry and the public.
- **Implement recommendations from the U.S. Government Accountability Office (GAO).** Standardize measurement across agencies and develop a single,

government-wide estimate of affected consumers and dollar losses, factoring in underreporting.[xxii]

Reforms Specific to Financial Services Policy

As part of a national strategy to combat scams, Aspen FSP's upcoming report will detail several reforms specifically relating to financial services, including:

- **Enhance information sharing efforts** to improve availability of actionable scam intelligence, by re-architecting the FinCEN SARS database to enable higher-volume and more automated data exchange and improving linkages with similarly revitalized FBI IC3 and FTC Sentinel databases.
- **Clarify or expand legal safe harbors** enabling financial institutions and non-financial institutions to exchange actionable scam intelligence and collaborate to prevent scams.
- **Establish parity of law enforcement powers across money movement**, including civil forfeiture of digital assets.
- **Enable risk-based payment pauses / limits** and other reasonable interventions to disrupt suspected malicious interactions.
- **Pilot bank-to-law enforcement victim report sharing**. Research shows that the vast majority of scam victims report the problem to their bank, while only a small portion report directly to a local or federal law enforcement agency.

Across the Ecosystem

All stakeholders should take a risk-based approach to flexibly prioritize interventions against the most impactful, and evolving, scam activities. Broader initiatives and cross-sector efforts should include:

- **Foster offensive technological innovation.** Use of artificial intelligence and advanced analytics is likely to be crucial for enhancing private and public sector capabilities in scam detection, prevention, and response.
- **Strengthen public awareness and consumer empowerment.** Study and improve consumer education, warning, and intervention practices. Increase funding for targeted, coordinated public awareness campaigns to help consumers recognize scams, reduce the stigma of victimization, and drive useful action such as reporting scams to a national law enforcement portal.
- **Assess potential benefits of establishing a U.S. National Anti-Scam Center.** Commission a study to determine the merits of creating a national hub that combines a reporting portal with professional training, public awareness, and victim support resources. A useful example of something similar is the National

Center for Missing and Exploited Children (NCMEC), a private non-profit organization established by President Ronald Reagan.

These and other recommendations are further explained in Aspen FSP's soon-to-be published report, a preview of which is attached to this letter as an appendix. The report is titled "United We Stand: A National Strategy to Prevent Scams. " It presents recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States. Aspen FSP will publish the report in early October of this year. We would be happy to brief Committee members and staff upon its release.

Appendix: Understanding Scam Trends

We are seeing increased, record-breaking losses to fraud and scams across the board

- Last year, the FBI received over 850,000 fraud and cybercrime complaints, with losses hitting a record $16.6 billion, a 33% increase over 2023.[xxiii]
- The biggest financial toll came from investment scams, at over $6.5 billion. This was followed by business email compromise at $2.77 billion and tech support fraud at $1.46 billion.[xxiv]
- The most common scam types were phishing, spoofing, extortion, and personal data breaches. [xxv]

Older Americans are continuing to bear the financial greater financial cost of fraud and scams while younger Americans experience them more frequently

- In 2024, Americans aged 60+ filed 147,000 complaints with the FBI, the highest of any age group, and suffered $4.9 billion in losses—with an average loss of $83,000.[xxvi]
- The FBI notes that over 33,000 seniors were targeted through crypto scams on phones and apps, leading to $2.8 billion in losses.[xxvii]
- People aged 70+ file half as many reports with losses compared to young adults, but their total losses are nearly 1.5 times greater than those of young people.[xxviii]

Call center, imposter, and AI-generated scams are scaling fast

- Call center scams—especially targeting seniors—remain one of the most lucrative and destructive tactics. In 2024, call center scams led to $1.9 billion in losses, often through impersonation of tech support or government agencies.[xxix]
- The FTC also reported that imposter scams, including romance, tech support, and government impersonation, led to $2.95 billion in losses, with a median loss of $800.[xxx]
- The FBI warned that criminals are increasingly exploiting artificial intelligence to create more convincing scams with less effort, using AI-generated images, audio, and video to impersonate trusted sources and deceive victims at scale.[xxxi]

Appendix: Preview of Forthcoming Report

"United We Stand: A National Strategy to Prevent Scams" (Preview)

The following is a preview of recommendations that Aspen FSP will publish in early October, 2025. The report presents recommendations for government and private sector collaboration to combat fraud against consumers, cut off criminal funding, and protect the United States.

Part One of the report is tactical, suggesting company and government agency actions to suppress scam activity and respond to it, at each stage of the fraud lifecycle. Part Two is structural, suggesting public policy and corporate practice reforms to empower scam prevention efforts. Each recommendation will offer one or more principles to guide action, paired with a set of "practical next steps and possible solutions" to give practitioners concrete ideas to test or implement.

Below is the report's Table of Contents for reference.

Endnotes

[i] To see a full list of member institutions, visit https://fraudtaskforce.aspeninstitute.org/membership

[ii] Jeffrey Gottfried, Eugenie Park, and Monica Anderson, "Online Scams and Attacks in America Today." Pew Research Center, July 31, 2025. https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/. A ratio of 1 in 5 adults equates to approximately 53 million adults, based on a total U.S. adult population of approximately 267 million. See: U.S. Census Bureau, "National Population by Characteristics: 2020-2024," June 2025. https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html.

[iii] Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."

[iv] Many fraud victims do not report their crimes due to feelings of shame, guilt, or embarrassment, doubts about their own judgment, fear of others' reactions, or belief that their losses are too small or that law enforcement will not act. Victims often blame themselves, even though skilled perpetrators are responsible. See, e.g., U.S. Department of Justice, Western District of Washington. "Financial Fraud Crime Victims." Last modified January 30, 2025. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud. Victim-blaming culture aimed at financial fraud victims, exacerbates victims' deep sense of shame and low self-esteem and shifts the focus away from perpetrators. See, e.g., AARP Fraud Watch Network and FINRA Investor Education Foundation, in collaboration with Heart + Mind Strategies. "Blame and Shame in the Context of Financial Fraud: A Movement to Change Our Societal Response to a Rampant and Growing Crime." June 2022. https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf.

[v] The 2024 Internet Crime Report combines information from 859,532 complaints of suspected internet crime and details reported losses exceeding $16 billion—a 33% increase in losses from 2023.
See: Federal Bureau of Investigation. "Internet Crime Report 2024." Internet Crime Complaint Center (IC3). April 24, 2025. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report. Of the 2.6 million fraud reports, 38% indicated money was lost. In 2024, people reported losing over $12 billion to fraud–an increase of over $2 billion over 2023. See: Federal Trade Commission. "Sentinel Network Data Book 2024." March 2025. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024 .

[vi] Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."

[vii] The rise of online scams represents a substantial transfer of wealth from middle-class households to organized criminal networks. See, e.g., The Economist. "Online Scams May Already Be as Big a Scourge as Illegal Drugs." February 6, 2025. https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs.

[viii] Reported scams in the U.S. rose between 2020 and 2024, with consumer complaints increasing from 4.7 million to 6.5 million and fraud losses growing from $3.3 billion to $12.5 billion (see, e.g., Federal Trade Commission 2020; 2024). U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2020." Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf. U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2024." Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

[ix] National Consumers League. "Top Ten Scams of 2024." January 16, 2025. https://nclnet.org/wp-content/uploads/2025/01/Top-Scams-of-2024.pdf.

[x] Younger households report experiencing scams at higher rates compared to older adults. According to a Gallup poll conducted in 2023, 22% of adults under 30 reported that someone in their household had fallen victim to a scam in the past year. This is notably higher than the 9% reported by those aged 50–64 and the 13% by those aged 65 and older. See, e.g., Gallup. "Scams Relatively Common, Anxiety-Inducing for Americans." July 31, 2023. https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx. Seniors reported $1.18 billion in fraud losses, compared to $810 million reported by adults in their 30s. Despite the higher financial losses among seniors, the number of fraud reports from both age groups was similar, indicating that seniors are losing approximately 50% more per incident than their younger counterparts.

See, e.g., U.S. Federal Trade Commission. "Consumer Sentinel Network Data Book 2024."
[xi] Gottfried, Park, and Anderson, "Online Scams and Attacks in America Today."
[xii] Ibid.
[xiii] Gallup. "Scams: Relatively Common and Anxiety-Inducing for Americans."
[xiv] Fulford, Scott. "More Than a Quarter of Americans Lost Money to Financial Fraud." *LinkedIn*, August 2025. https://www.linkedin.com/pulse/more-than-quarter-americans-lost-money-financial-fraud-scott-fulford-2qije. Estimates were calculated using the publicly accessible CFPB 2024 Making Ends Meet Survey data: https://www.consumerfinance.gov/data-research/making-ends-meet-survey-data/.
[xv] Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." March 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.
[xvi] TRM Labs. "All Roads Lead to China: North Korean Hackers, Fentanyl, Cartel Money Laundering, and Global Organized Crime." May 27, 2025. https://www.trmlabs.com/resources/reports/all-roads-lead-to-china. See also: Ken Westbrook, "As Scams by Foreign Organized Crime Soar, Here's How America Must Respond" (Stop Scams Alliance, December 2024), accessed September 3, 2025, PDF, 4-5.
[xvii] "Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams" U.S. Department of the Treasury press release, September 8, 2025. https://home.treasury.gov/news/press-releases/sb0237
[xviii] "Treasury Sanctions the Zhao Wei Transnational Criminal Organization" U.S. Department of the Treasury press release, January 30, 2018. https://home.treasury.gov/news/press-releases/sm0272
[xix] "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups" U.S. Department of the Treasury press release, September 13, 2019. https://home.treasury.gov/news/press-releases/sm774
[xx] "Mexican Cartels Target Americans in Timeshare Fraud Scams, FBI Warns" FBI News Story, June 7, 2024. https://www.fbi.gov/news/stories/mexican-cartels-targeting-americans-in-timeshare-fraud-scams-fbi-warns
[xxi] "Fraud and Scam Measurement Framework". Aspen Institute National Task Force on Fraud and Scam Prevention. https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/6830b13e294cb446da01973d/1748021566525/MeasurementFramework_5-23-25.pdf
[xxii] "Consumer Protection: Actions Needed to Improve Complaint Reporting, Consumer Education, and Federal Coordination to Counter Scams" Government Accountability Office, April 8, 2025. https://www.gao.gov/products/gao-25-107088
[xxiii] FBI, 2024 Internet Crime Report, p. 4.
[xxiv] Ibid, p. 10
[xxv] Ibid, p. 9
[xxvi] Ibid, p. 27
[xxvii] FBI, 2024 Internet Crime Report, p. 35.
[xxviii] FTC, Consumer Sentinel Network Data Book 2024, p. 6.
[xxix] FBI, 2024 Internet Crime Report, pp. 11, 14.
[xxx] FTC, Consumer Sentinel Network Data Book 2024, p. 8.
[xxxi] FBI Alert Number: I-120324-PSA, 2024